PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/38, H04L 9/32

A1

(11) International Publication Number: WO 97/15161

(43) International Publication Date: 24 April 1997 (24.04.97)

(21) International Application Number: PCT/FI96/00543

(22) International Filing Date: 16 October 1996 (16.10.96)

(30) Priority Data:
08/544,199 17 October 1995 (17.10.95) US

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Upseerinkatu 1, FIN-02600 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: MURTO, Juhani [FI/US]; 758 Swallow Drive, Coppel, TX 75019 (US).

(74) Agent: OY KOLSTER AB; Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI).

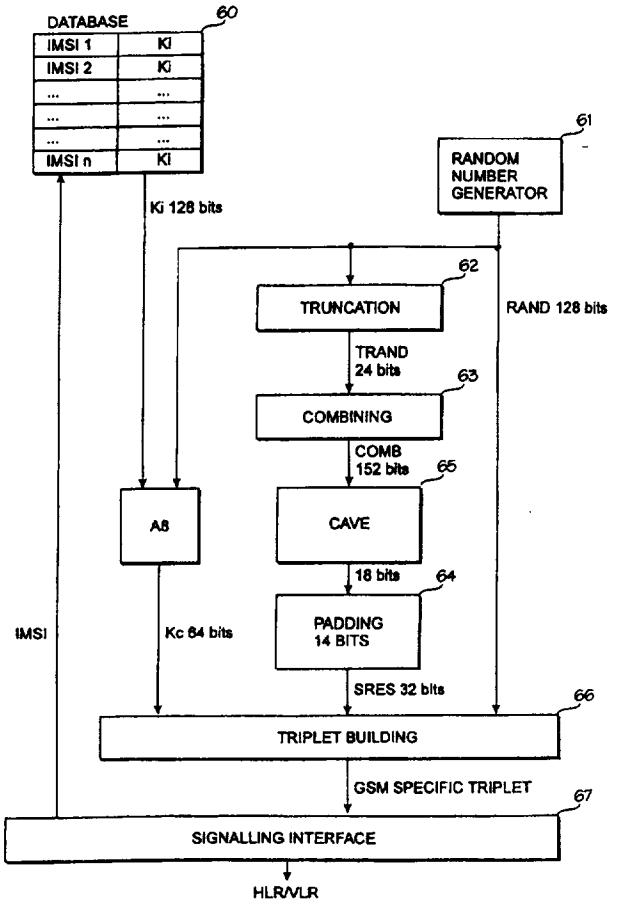
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SUBSCRIBER AUTHENTICATION IN A MOBILE COMMUNICATIONS SYSTEM

(57) Abstract

An authentication in a GSM based mobile comunications system relies on a challenge and response principle. A 32-bit Signed Response (SRES) parameter is calculated by A3 algorithm from a 128-bit Random Number (RAND) and a 128-bit Authentication Key K_i in a mobile station and in an authentication center, and the SRES values are compared. A CAVE algorithm having a 152-bit input parameter and an 18-bit output parameter is employed as the A3 algorithm. Paramater adaptation functions are provided between the input parameter of the CAVE algorithm and the GSM type input parameters, namely the random number RAND and the authentication key K_i, as well as between the output parameter of the CAVE algorithm and the GSM output parameter, namely the signed response SRES.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Subscriber authentication in a mobile communications system

Field of the invention

The present invention relates to security functions in mobile communications networks, and particularly to a subscriber authentication in mobile communications networks.

Background of the invention

In all telecommunication networks both the users and the network operator have to be protected against undesirable intrusion of third parties as far as possible. Thus several kinds of security functions are needed in the networks. The major aspects of the network security are 1) the protection of the information that the network conveys; and 2) authentication and access control of the users of the network. The major security mechanism for the protection of information is, and is likely to remain, some form of encryption. Authentication is a means of trying to ensure that information comes from the source it is claimed to come from. It is typically based on passwords and keys. Access rights are assigned in terms of the ability to send and/or receive via the transmission medium. Also access mechanisms typically depend on some form of password or key.

Due to the use of radio communications for transmissions to the mobile subscribers, radio accessed networks, such as Public Land Mobile Networks (PLMN), are particularly sensitive to misuse of their resources by unauthorized users and eavesdropping on the information which is exchanged on the radio path. This comes from the possibility to listen to and transmit radio signals from anywhere, without tampering with user's or operator's equipment. It can be seen that

PLMNs have a need for a higher level of security than traditional telecommunication networks.

The pan-European digital cellular radion which is known as GSM (Global System for Mobile Communications) contains a highly secure authentication system. It is based on socalled challenge and response principle. At subscription time a secret number called a Subscbiber Authentication Key (K_i) is allocated to the subscriber together with an International Mobile Subscriber Identity (IMSI). K_i is stored in a special purpose element of the GSM network, called an Authentication Center (AUC) which is associated with or linked to a Home Location Register (HLR) of the subscriber. AUC contains also a ciphering algorithm, called A8, and an authentication algorithm, called A3, as well as a generation of random numbers RAND. A parameter called a ciphering key K_c is generated from K_i and RAND by the algorithm A8. Similarly, a parameter called a Signed Response SRES is generated from K_i and RAND by the algorithm A3. The three parameters RAND, K_c and SRES make up a "triplet" specific of a subsriber to be used for further authentication and ciphering. In order to avoid calculation and transfer of triplet every time it is needed, several triplets are calculated in advance for each subscriber by AUC/HLR and on request delivered to a Visitor Location Register VLR and a Mobile Services Switching Center (MSC) there they are stored. MSC/VLR will always have at least one triplet unused for each of its visitor subscribers. Tight security requires that a triplet is used only once, for one communication, and is then destroyed. When a subscriber has used all it's available triplets, the AUC/HLR is then requested to calculate and send back a new series.

A GSM mobile station is split into two parts, one which contains the hardware and software specific to the

radio interface, the mobile equipment, and and another which contains the subscriber specific data: the Subscriber Identity Module or SIM. Each subscriber has the SIM, typically in a form of a smart card, which takes responsibility for most of the security functions at the mobile station side. It stores K_i, the authentication algorithm A3 and the ciphering algorithm A8, as well as the ciphering key K_c received from the network side.

During authentication, the VLR/MSC sends the random number RAND (and also K_c) of the triplet to the mobile station. The mobile station, more particularly the SIM, processes RAND using the authentication algorithm A3 and the authentication key K_i, and returns the resulting Signed Response SRES to the VLR/MSC. This SRES is checked against the SRES of the triplet given by the HLR to. If the two SRESes are equal to each other, the access is allowed, and otherwise denied.

All the security mechanism in the GSM rely on secrecy of authentication key K_i. K_i is never transmitted and never leaves the AUC/HLR. Also the SIM protects completely K_i against reading. Because the mathematical algorithm A3 works only one way (one-way trap door function) it is impossible to derive the key K_i from the RAND-SRES pairs transmitted. Further the authentication algorithm A3 itself is a secret algorithm, it can not be found even in the GSM specifications. The specifications only require that computation of K_i knowing RAND and SRES should be as complex as possible. This level of complexity determines which security level has been achieved. Beyond this requirement, the only constraint imposed on A3 is the size of the input parameter (RAND is 128 bits long) and the size of the output parameter (SRES must be 32 bits long). K_i can be of any format and lenght when stored in Auc/HLR, only if K_i would be

transported in the network it would be constrained to a maximum lenght of 128 bits. In fact, the design choices of GSM, both in the mobile station and in the infrastructure, make it possible for the operators to choose the A3 applicable to their own subcsribers independently from other operators.

In the U.S.A a digital cellular system called Personal Communications System (PCS) is under development. The US PCS is based on the GSM system in a great extent, especially as regards network architecture and protocols, including the security functions. However, some minor modifications are being made in various parts of the system. One potential modification might be that authentication algorithm A3 used in the GSM system would be replaced by CAVE algorithm in the US PCS since the CAVE algorithm has been developed in the USA and is already used in analog AMPS networks (Advanced Mobile Phone Service). The CAVE algorithm which might be suitable to be used for authentication in the PCS system would have an 152-bit input parameter consisting of a number of concanated information fields, and a 18-bit output parameter, whereas the A3 algorithm in the GSM has the 128-bit K_i and RAND parameters as input parameters and 32-bit SRES parameter as an output parameter. Therefore, replacement of A3 with the CAVE algorithm in a GSM based mobile communications system is not possible without further modifications. However, modifications may easily affect in various protocols, functions, messages and data structures throughout the system and thereby make the CAVE algorithm technically and economically inattractive. A further disadvantage is that the compability with the GSM system will be lost, and consequently, for example, SIM roaming between the GSM and US PCS systems will not be possible.

Summary of the Invention

An object of the invention is to enable the use of the CAVE algorithm as the A3 algorithm in the GSM system or in a GSM based mobile communications network without incurring modifications in GSM authentication parameters.

A further object of the invention is to enable the use of the CAVE algorithm as the A3 algorithm in the GSM system or in a GSM based mobile communications network without modifications in the GSM triplet data structure.

A still further object of the invention is to enable the use of the CAVE algorithm as the A3 algorithm in the GSM system or in a GSM based mobile communications network but otherwise retain the security functions of the standard GSM system.

One aspect of the invention is an authentication method for a mobile communications network, comprising steps of

utilizing an authentication procedure intended to be used with a first authentication response calculation method,

utilizing a second authentication response calculation method instead of said first authentication response calculation method,

providing an authentication key compatible with said first authentication response calculation method but incompatible with said second authentication response calculation method, for each subscriber of said mobile communications network,

generating a random number compatible with said first authentication response calculation method but incompatible with said second authentication response calculation method,

deriving an input parameter compatible with said

second authentication response calculation method from said authetication key and said random number,

calculating by said second autentication response calculation method an authentication response incompatible with a authentication response format of said authentication prosedure utilized in said mobile communications network,

modifying said authentication response into a format compatible with said authentication response format of said authentication procedure,

transferring and storing said authentication response in said mobile communications network in said format compatible with said authentication procedure.

According to the invention parameter adaptation functions are provided between the input parameter of the CAVE algorithm and the GSM type input parameters, namely the random number RAND and the authentication key K_i, as well as between the output parameter of the CAVE algorithm and the GSM output parameter, namely the signed response SRES. As a result no modifications are needed in the CAVE algorithm itself, nor it is necessary to depart from the GSM type security functions elsewhere than in the calculation of SRES in the authentication center AUC/HLR and in the mobile station MS.

Brief Description of the Drawings

The preferred embodiments of the invention will be described with reference to attached drawing, wherein

Fig. 1 is a block diagram illustrating a GSM based cellular mobile radio system,

Fig. 2 is a functional block diagram of the prior art authentication and ciphering parameter processing unit in the authentication center AUC,

Fig. 3 is a functional block diagram of the prior art authentication and ciphering parameter processing unit in the mobile station MS,

Fig. 4 is a functional block diagram of the the authentication and ciphering parameter processing unit in the MSC/VLR,

Fig. 5 illustrates the signalling related to the generation, transfer and use of the authentication and ciphering parameters,

Fig. 6 is a functional block diagram of the authentication and ciphering parameter processing unit according to the invention in the authentication center AUC,

Fig. 7 is a functional block diagram of the authentication and ciphering parameter processing unit according to the invention in the mobile station MS.

Preferred Embodiments of the Invention

The present invention can be applied in the Paneuropean digital mobile radio system GSM or in any GSM based mobile radio system, such as DCS1800 digital communication system and the U.S. digital cellular system called Personal Communication System (PCS). Although the preferred embodiment of the invention will be described as an application in a standard GSM system in the following, the primary field of the application will apparently be the PCS system in the U.S.A. The structure and operation of the GSM system are well known to one skilled in the art and defined in the GSM specifications issued the European Telecommunications Standards Institute ETSI. A reference is also made to the GSM system for a mobile communications, M.Mouly & M.Pautet, Palaiseau, France, 1992; ISBN2-9507190-0-7.

The basic structure of GSM system is shown in Figure 1.

The GSM structure consists of two parts: the base station subsystem (BSS), and the network subsystem (NSS). The BSS and the mobile stations MS communicate via radio connections. In the BSS, each cell is served by a base transceiver station (BTS). A group of BTS is connected to a base station controller (BSC) whose function is to manage the radio frequencies and channels used by the BTS. The BSCs are connected to a mobile switching centre (MS). The MSC is for switching calls involving at least one mobile station MS. Certain MSCs are connected to other telecommunication networks such as the public switched telephone network (PSTN), and contain gateway functions for handling calls to and from these networks. These MSCs are known as gateway MSCs (GMSCs).

There are two main types of database concerned with the routing of calls. There is a home location register (HLR) that stores subscriber data on all the subscribers of the network on a permanent or semipermanent basis, including information on the services to which the subscriber may have access, and the current location of the subscriber. The second type of register is the visitor location register (VLR). The VLR is attached generally to one MSC, but it may, however, serve several MSCs. It is common practice that VLR is integrated into the MSC. This integrated network element is known as visitor MSC (VMSC). Whenever a mobile station MS is active (logged on and able to make or receive a call) most of the mobile subscriber data about a mobile station MS that is held in the HLR is downloaded (copied) into the VLR of the MSC in whose area the mobile MS is.

As noted above, in the mobile radio service, great care must by taken to prevent unauthorized call attempts and intrusion or listening-in by third parties.

Protection mechanisms in GSM system authenticate the calling or called mobile station, and use ciphering key to encode speech and data on the traffic channel.

The prior art mechanism according to the GSM specifications for providing authentication and ciphering keys will now be described with reference to Figures 2, 3, 4 and 5.

At subscription time a secret number called a subscriber authentication key (K_i) is allocated to the mobile subscriber together with an international mobile subscriber identity (IMSI). As shown in Figure 2, the authentication centre AUC comprises a database 20 which stores the authentication key K_i for each mobile subscriber in the GSM network. K_i of the mobile subscriber can be retrieved from the database 20 using the IMSI of the mobile subscriber as an index. The AUC is further provided with an ciphering algorithm A8, an authentication algorithm A3, and a random number generator 21. The random number generator 21 provides random numbers RAND having length of 128 bits. The key K_i retrieved from database 20 and the random number RAND from the random number generator 21 are used as input parameters in the authentication algorithm A3 to calculate the signed response SRES, and as input parameters in ciphering algorithm A8 to calculate the ciphering key K_c for traffic channel encoding. The three parameters RAND, SRES and K_c make up a triplet for a mobile subscriber.

The triplets will be transferred further to the visited MSC/VLR to be used for authentication and ciphering as will be explained in more detail below.

A triplet is used only once, for one communication, and is then destroyed. In order to avoid calculation and transfer of triplet every time it is needed, several triplets are calculated in advance for

each mobile subscriber by AUC/HLR and on request delivered to the visited MSC/VLR where they are stored.

The visited MSC/VLR stores a reserve of a few of such triplets per subscriber to be retrieved at need. Referring to Fig. 4, there is shown an example of a security parameter file 40 maintained in the visited MSC/VLR. The file 40 contains n triplets 1...n for each IMSI (subscriber).

This reserve in the security parameter file 40 is first established when the mobile subscriber first registers in the visited MSC/VLR: it is part of the subscriber data downloaded from the HLR in the INSERT SUBSCRIBER DATA message. When a subscriber has used all it's available triplets, the AUC/HLR is then requested to calculate and send back a new series. Referring to Fig. 5, this triplet replenishing produce consist of two messages: SEND PARAMETERS message and it's answer, SEND PARAMETERS RESULT message. The former message contains the IMSI of the mobile subscriber which is used to retrieve the K_i for calculation of the triplets as described above with reference to Fig. 2. The calculated triplets will be delivered to the MSC/VLR in the SEND PARAMETERS RESULT message and stored in the VLR.

Referring further to Fig. 4, the mobile station MS sends an access request to the MSC/VLR. The MSC/VLR retrieves one of the triplets reserved for the subscriber of the mobile station MS in the security parameter file using the IMSI as an index. The MSC/VLR conveys on one hand the value of K_c to the channel equipment in the BSC to be used in the traffic channel ciphering, and on the other hand the value of RAND to the MS in the AUTHENTICATION REQUEST message, as shown by block 41 in Fig. 4. On basis of the RAND the mobile station MS calculates the other values of the triplet (SRES and K_c).

Referring to Fig. 3, the MS stores a copy of the ciphering key K_i of the mobile subscriber, as well as the ciphering algorithm A8 and the authentication algorithm A3. On receiving the AUTHENTICATION REQUEST message for the MSC/VLR, the MS extracts the RAND from the message, and then inputs the RAND and the stored K_i to the algorithms A3 and A8. For calculating the signed response SRES and the ciphering key K_c, respectively. The calculated SRES will be conveyed to the MSC/VLR in the AUTHENTICATION RESULT message for completing the authentication as shown in Figs. 4 and 5.

Referring to Fig. 4, the MSC/VLR extracts the value of SRES from AUTHENTICATION RESULT message (block 42) and retrieves the stored value of SRES from the file 40 (block 43). Then, for this communication, prior to any other processing, the MSC/VLR "authenticates" the mobile subscriber by checking that the SRES calculated in the AUC/HLR is identical to the SRES calculated in the MS (block 44). If the two values are identical, the access is granted (block 45). If the two values are not identical, the access is denied (block 46).

The ciphering procedure is not relevant to the present invention and will not be described in more detail herein.

As noted in the background art of the invention, it might be a need to use the CAVE algorithm as the authentication algorithm A3 in the USA a digital cellular system called Personal Communications System (PCS), or other cellular systems based on the GSM system in a great extent, especially as regards network architecture and protocols, including the security functions. The CAVE algorithm has been developed in the USA and the availabilily of the CAVE algorithm information is governed under ITAR (U.S. International Traffic and Arms Regulation). However, the CAVE is

already used in analog AMPS networks (Advanced Mobile Phone Service) and its input/output parameters are specified in EIA/TIA srandard IS-54. The CAVE algorithm has an 152-bit input parameter consisting of a number of concanated information fields, and a 18-bit output parameter. Problems are, however, encountered in the practical implementation due to the fact that the A3 algorithm in the GSM system has the 128-bit K_i and RAND as input parameters and 32-bit SRES as an output parameter.

These problems will be overcome when, according to the present invention, an adaptation of the parameters is made at the input and output of the CAVE algorithm. As a result, no modifications are needed in the CAVE algorithm itself, nor it is necessary to depart from the GSM specifications elsewhere than in the calculation of SRES in the AUC/HLR and the MS.

The preferred embodiments of the parameter adaptation according to the invention will now be described with reference to Figs. 6 and 7.

Referring now to Fig. 6, the authentication centre AUC according to the invention comprises a database 60 and a random number generator 61 which are similar to the database 20 and generator 21 shown in Fig. 2. The database 60 stores the 128-bit authentication keys K_i according to the GSM specifications for all mobile subscribers of the GSM network, indexed by the IMSIs. The IMSI by which the K_i is selected for furher calculation is receide from a signalling interface 67 which receives it from HLR or VLR, eg. in the SEND PARAMETERS message. The random number generator 61 provides the 128-bit random numbers RAND in accordance with the GSM specifications.

The K_i and RAND are inputs to the ciphering algorithm A8 which calculates the 64-bit ciphering key K_c

in accordance with the GSM specifications. In other words, the calculation of K_c is identical to that described with reference to Fig. 2.

The 128-bit RAND is also an input to a truncation unit 62 which truncates the RAND into 24-bit truncated RAND (TRAND). The TRAND may contain, for example, 24 most significant bits of RAND. It is appreciated, however, that the truncation operation as used herein is intended to cover any method to derive 24-bit random number TRAND from the 128-bit random number RAND. It should be noted that although the lenght of K_i is 128 bits in the preferred embodiment, it may have any length of N bits, where N is integer less than or equal to 128. Consequently, lenght M of TRAND depends on N, being M=152-N bits.

The 24-bit TRAND is then inputted to a combining unit 63, the other input of unit 63 being the 128-bit authentication key K_i. The output of the combining unit 63 is a 152-bit combination COMP of K_i and TRAND. The 128 most significant bits of the COMP may contain the K_i and the 24 least significant bits may contain the TRAND. It is appreciated, however, that the combination operation as used herein is intended to cover any method, e.g. a logical operation, to derive 152-bit value by combining K_i and TRAND.

The 152-bit COMP parameter meets the requirements set on the input parameter of the CAVE algorithm in the calculation unit 65. Thus, the parameter adaptation according to the invention derives a CAVE compatible input parameter from the GSM compatible input parameters K_i and RAND. As a result of the calculation, the CAVE calculation unit 65 outputs a 18-bit output parameter.

The 18-bit output parameter from the CAVE is then inputted to the padding unit 64 in which 14 stuff bits will be inserted so as to obtain a 32-bit value. The 14

stuff bits may establish, for example, the 14 least significant bits of the 32-bit parameter, the 18 most significant bits containing the 18-bit output from CAVE 65. It is appreciated, however, that the padding operation as used herein is intended to cover any method, e.g. logical operation, to lengthen the 18-bit CAVE output parameter by 14 bits to obtain 32 bits.

The resulting 32-bit output parameter will be then used as the signed response SRES according to the GSM specifications. Thus, the parameter adaptation according to the invention derives a GSM compatible output parameter from a CAVE compatible output parameter.

The three GSM compatible security parameters SRES, K_c and RAND will be inputted to a triplet building unit 66 in which a standard GSM triplet is built. The triplet will be transferred to HLR or VLR via the signalling interface 67. Thus, the SRES will be transferred and processed in the GSM network in a similar manner as the standard SRES.

Referring now to Fig. 7, the mobile station MS according to the invention stores a copy of the ciphering key K_i of the mobile subscriber in a memory 75. The MS also comrises a calculation unit 76 carrying out the ciphering algorithm A8, and a calculation unit 77 carrying out the CAVE algorithm for authentication. On receiving the AUTHENTICATION REQUEST message from the MSC/VLR, the of the MS, which contains the hardware and software specific to the radio interface, the mobile equipment 78, extracts the RAND form the message, and then inputs the RAND and the stored K_i to the A8 calculation unit 76 for calculation of the ciphering key K_c. In the preferred embodiment of the invention all the functional blocks except 78 are located in the Subscriber Identity Module or SIM of the MS.

The 128-bit RAND is also an input to a truncation unit 72 which truncates the RAND into 24-bit TRAND. The truncation unit 72 is identical to the truncation unit 62 shown in Fig. 6.

The 24-bit TRAND is then inputted to a combining unit 73, together with the 128-bit K_i. The output of the combining unit 73 is a 152-bit COMP. The combining unit 73 is identical to the combining unit 63 shown in Fig. 6.

The 152-bit COMP is then inputted to the CAVE calculation unit 77 which outputs a 18-bit output parameter.

The 18-bit output parameter from the CAVE 77 is inputted to a padding unit 74 in which 14 stuff bits are attached so as to provide a 32-bit value. The padding unit 74 is identical to the padding unit 64 shown in Fig. 6.

The resulting 32-bit output parameter will be then used as the SRES parameter according to the GSM specifications. The SRES will returned to the mobile equipment 78 and sent further to the MSC/VLR in the AUTHENTICATION RESULT message and processed in the MSC/VLR as in the standard GSM system.

An example of alternative embodiments for deriving the 152-bit CAVE input parameter from the N-bit K_i and RAND parameters is shown in Fig. 8. In the following examples N=128 but it may be any positive integer in these embodiments. K_i will be divided into two parts: 104 bits of the K_i, e.g. 104 LSB bits, are inputted to an input of a logical unit 81. The remaining 24 bits of K_i are inputted to a combiner 82. Similarly, RAND will be divided into two parts: 104 bits of the RAND, e.g. 104 MSB bits, are inputted to the logical unit 81. The remaining 24 bits of RAND are inputted to another input of the combiner 82. A logical operation,

such AND, OR or exclusive OR (XOR), is performed between the two 104-bit inputs, and a single 104-bit output is provided. The 104-bit output from the logical unit 81 is inputted to the combiner 82. The combiner 82 assembles the two 24-bit inputs and the 104-bit input into a 152-bit parameter to be inputted to the CAVE algorithm. When applied in the authenticatication center of Fig. 6 and in the mobile station of Fig. 7, the logical unit 81 and the combiner 82 will substitute for the truncation unit 62,72 and the combiner 63,73, respectively.

As a further modification to the embodiment of the Fig. 8, the 104 bits of K_i and the 104 bits of RAND may be subdivided into equal number of subblocks, and different logical operations are performed between different subblocks. There may be four subsblocks of 26 bits, for example.

The drawing and the associated description is solely intended to ilustrate the present invention. Changes and modifications will apparent to a skilled person in the art without departing from the scope and spirit of the attached claims.

Claims

1. An authentication center for a mobile communications network, comprising

a database storing an authentication key for each subscriber of said mobile communications network, said authentication key being an input parameter for calculation of a ciphering key and an authentication response parameter and in a format required by a first authentication procedure,

a source of a random number, said random number being another input parameter for calculation of a ciphering key and an authentication response parameter and in a format required by said first authentication procedure,

an encryption key calculation unit having said authentication key from the database and a random number from said source of random numbers as input parameters and outputting a ciphering key in a format according to said first authentication procedure,

an authentication response parameter calculation unit requiring a single input parameter and outputting an authetication response parameter in a format other than the format of the authentication response parameter according to said first authentication procedure,

a first adaptation unit responsive to said authentication key and said random number as input parameters for providing said single input parameter to said authentication response calculation unit,

a second adaptation unit responsive to said authentication response parameter outputted by said authentication response parameter calculation unit for providing said authentication response parameter according to the first authentication procedure.

2. An authentication parameter processing unit in a mobile station, comprising

a memory storing an authentication key for a mobile subscriber using said mobile station, said authentication key being an input parameter for calculation of a ciphering key and an authentication response parameter and in a format required by a first authentication procedure,

a source of a random number, said random number being another input parameter for calculation of a ciphering key and an authentication response parameter and in a format required by said first authentication procedure,

an encryption key calculation unit having said authentication key from the database and a random number from said source of random numbers as input parameters and outputting a ciphering key in a format according to said first authentication procedure,

an authentication response parameter calculation unit requiring a single input parameter and outputting an authetication response parameter in a format other than the format of the authentication response parameter according to said first authentication procedure,

a first adaptation unit responsive to said authentication key and said random number as input parameters for providing said single input parameter to said authentication response calculation unit,

a second adaptation unit responsive to said authentication response parameter outputted by said authentication response parameter calculation unit for providing said authentication response parameter according to the first authentication procedure.

3. An authentication method for a mobile communications network, comprising steps of

utilizing an authentication procedure intended to

be used with a first authentication response calculation method,

utilizing a second authentication response calculation method instead of said first authentication response calculation method,

providing an authentication key compatible with said first authentication response calculation method but incompatible with said second authentication response calculation method, for each subscriber of said mobile communications network,

generating a random number compatible with said first authentication response calculation method but incompatible with said second authentication response calculation method,

deriving an input parameter compatible with said second authentication response calculation method from said authetication key and said random number,

calculating by said second autentication response calculation method an authentication response incompatible with a authentication response format of said authentication prosedure utilized in said mobile communications network,

modifying said authentication response into a format compatible with said authentication response format of said authentication procedure,

transferring and storing said authentication response in said mobile communications network in said format compatible with said authentication procedure.

4. An authentication method for a GSM based mobile communications network, comprising steps of

utilizing a GSM based authentication procedure intended to be used with a GSM based authentication response calculation method, said GSM based authentication response calculation method comprising 128-bit random number RAND and N-bit authentication key

K_i as input parameters and a 32-bit signed response SRES as an output parameter, N being a positive integer,

utilizing a CAVE calculation method as an authentication response calculation method instead of said GSM based authentication response calculation method, said CAVE method comprising a 152-bit input parameter and a 18-bit output parameter,

providing unique value of said N-bit K_i for each subscriber of said mobile communications network,

storing said values of K_i in a database in an authentication center,

receiving a request to provide said SRES for one of said mobile subscribers,

retrieving said N-bit K_i of said one of said mobile subscribers from said database,

generating said 128-bit RAND,

deriving said 152-bit input parameter from said N-bit K_i and 128-bit RAND,

calculating by said CAVE calculation method said 18-bit output parameter,

padding 14 additional bits into said 18-bit output parameter to obtain said 32-bit SRES,

transferring and storing said 32-bit SRES in said GSM based mobile communications network according to said GSM based authentication procedure.

5. A method according as claimed in claim 4, wherein said step of deriving comprises steps of

truncating said 128-bit RAND into (152-N)-bit truncated RAND, N being an integer less than or equal to 128,

combining said (152-N)-bit truncated RAND with said N-bit K_i to obtain said 152-bit input parameter.

6. An authentication method for a GSM based mobile communications network, comprising steps of

utilizing a GSM based authentication procedure

intended to be used with a GSM based authentication response calculation method, said GSM based authentication response calculation method comprising 128-bit random number RAND and N-bit authentication key K_i as input parameters and a 32-bit signed response SRES as an output parameter, N being a positive integer,

utilizing a CAVE calculation method as an authentication response calculation method instead of said GSM based authentication response calculation method, said CAVE method comprising a 152-bit input parameter and a 18-bit output parameter,

storing an unique value of said N-bit K_i provided for a mobile subscriber in a memory of a mobile station,

receiving from a base station by said mobile station an authentication request including said 128-bit RAND,

retrieving said N-bit K_i from said memory,

deriving said 152-bit input parameter from said N-bit K_i and 128-bit RAND,

calculating by said CAVE calculation method said 18-bit output parameter,

padding 14 additional bits into said 18-bit output parameter to obtain said 32-bit SRES,

transmitting said 32-bit SRES to said base station.

7. A method according as claimed in claim 6, wherein said step of deriving comprises steps of

truncating said 128-bit RAND into (152-N)-bit truncated RAND, N being an integer less than or equal to 128,

combining said (152-N)-bit truncated RAND with said N-bit K_i to obtain said 152-bit input parameter.

8. An authentication parameter calculation unit for a mobile communication system, comprising

a CAVE algorithm calculator having a first input

for receiving a 152-bit input parameter, and an output for outputting a 18-bit output parameter,

a first adaptor having a first input for receiving 128-bit random number RAND, a second input fo receiving a N-bit authentication key K_i, and an output for outputting said 152-bit input parameter derived from said N-bit K_i and 128-bit RAND to said input of said CAVE algorithm calculator, N being a positive integer,

a second adaptor having an input for receiving said 18-bit output parameter CAVE algorithm calculator, and an output for outputting a 32-bit signed response SRES, wherein K_i, RAND and SRES are GSM-based authentication parameters.

Fig. 1
(PRIOR ART)

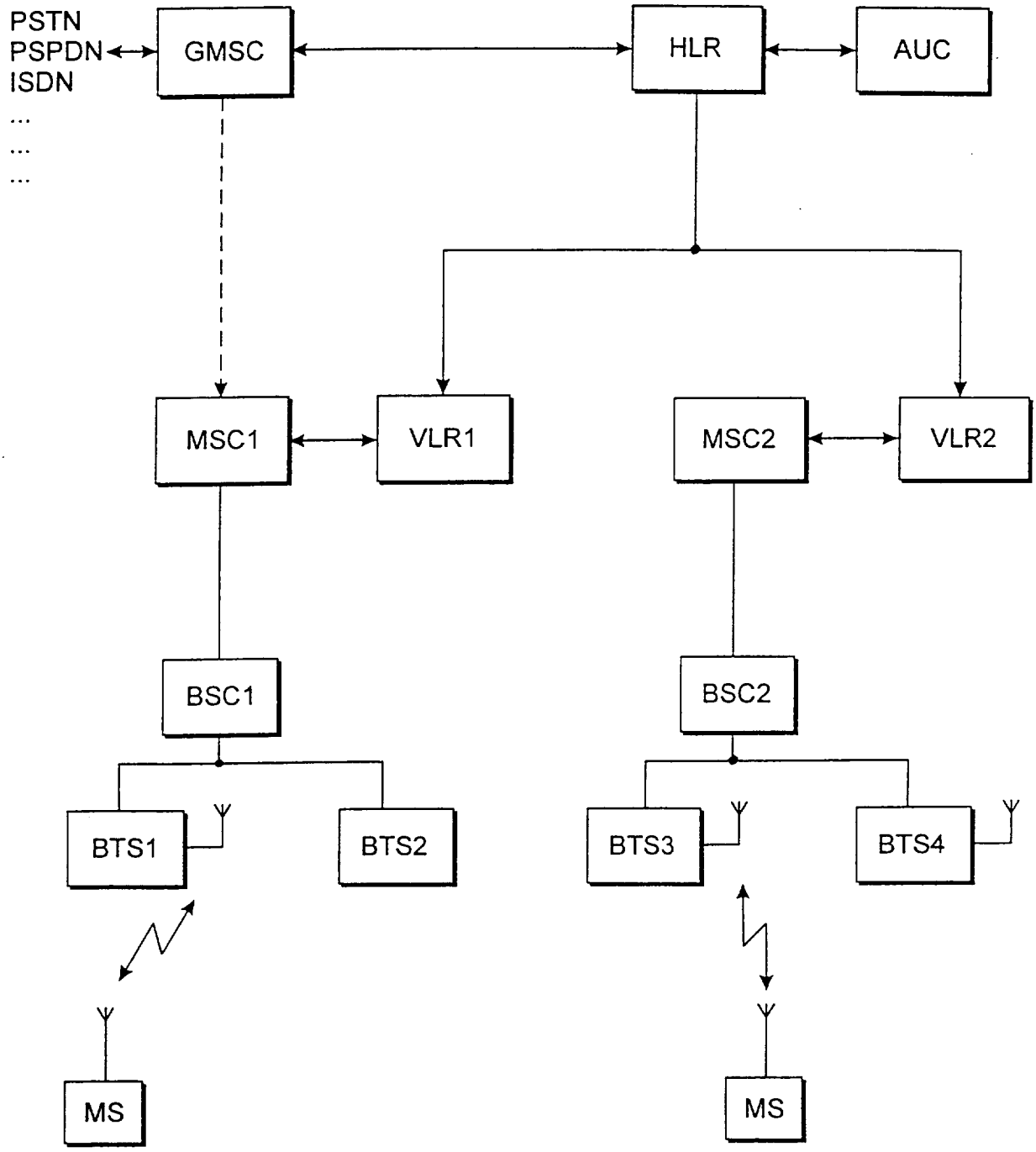


Fig. 2

(PRIOR ART)

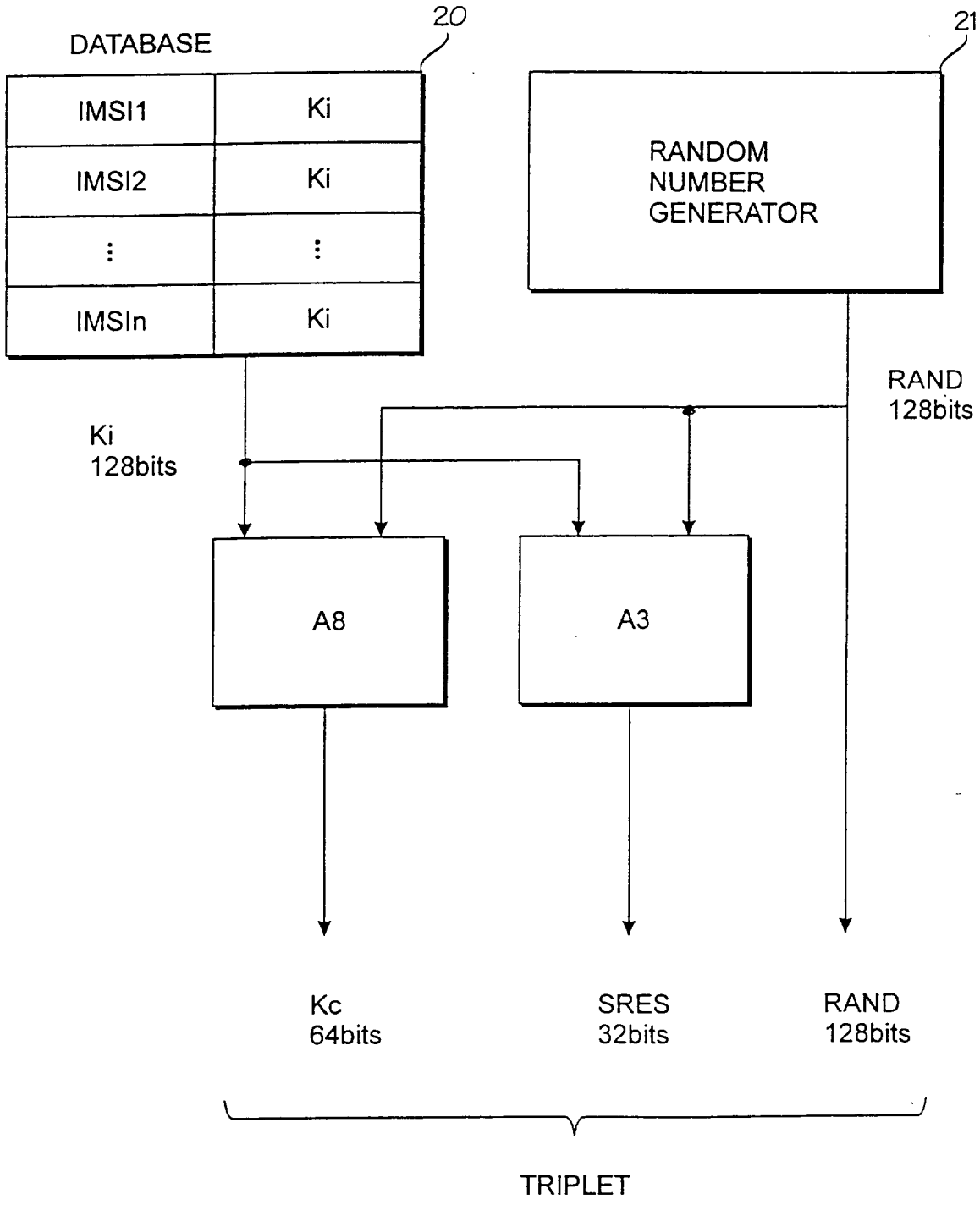


Fig. 3
(PRIOR ART)

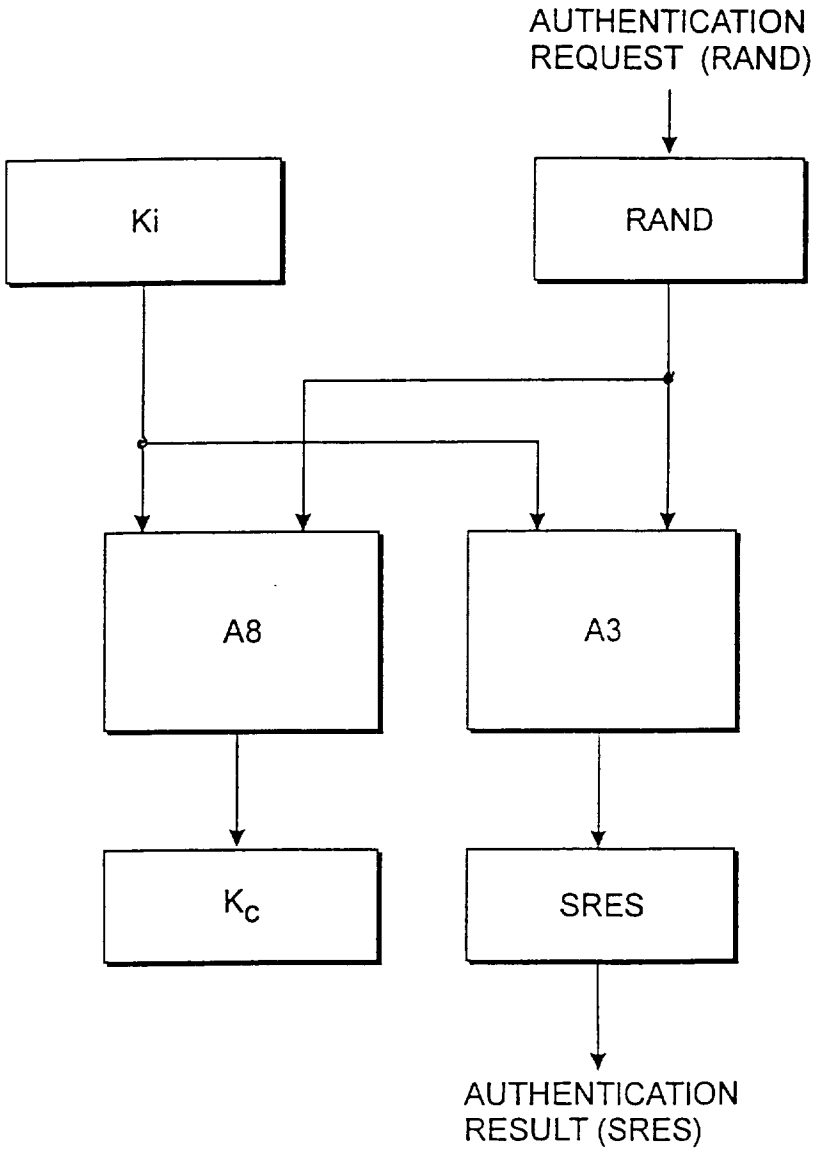


Fig. 4
(PRIOR ART)

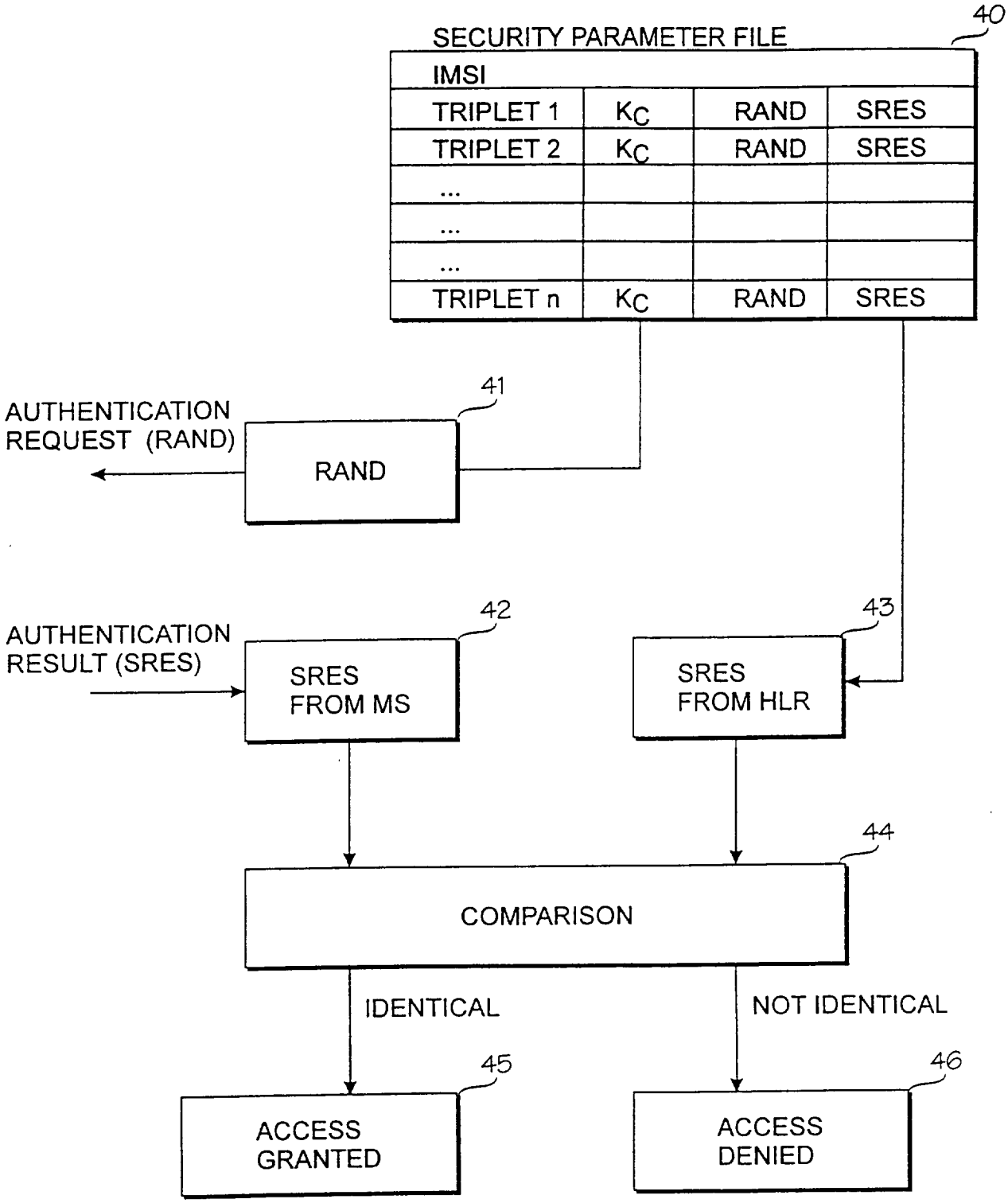


Fig. 5
(PRIOR ART)

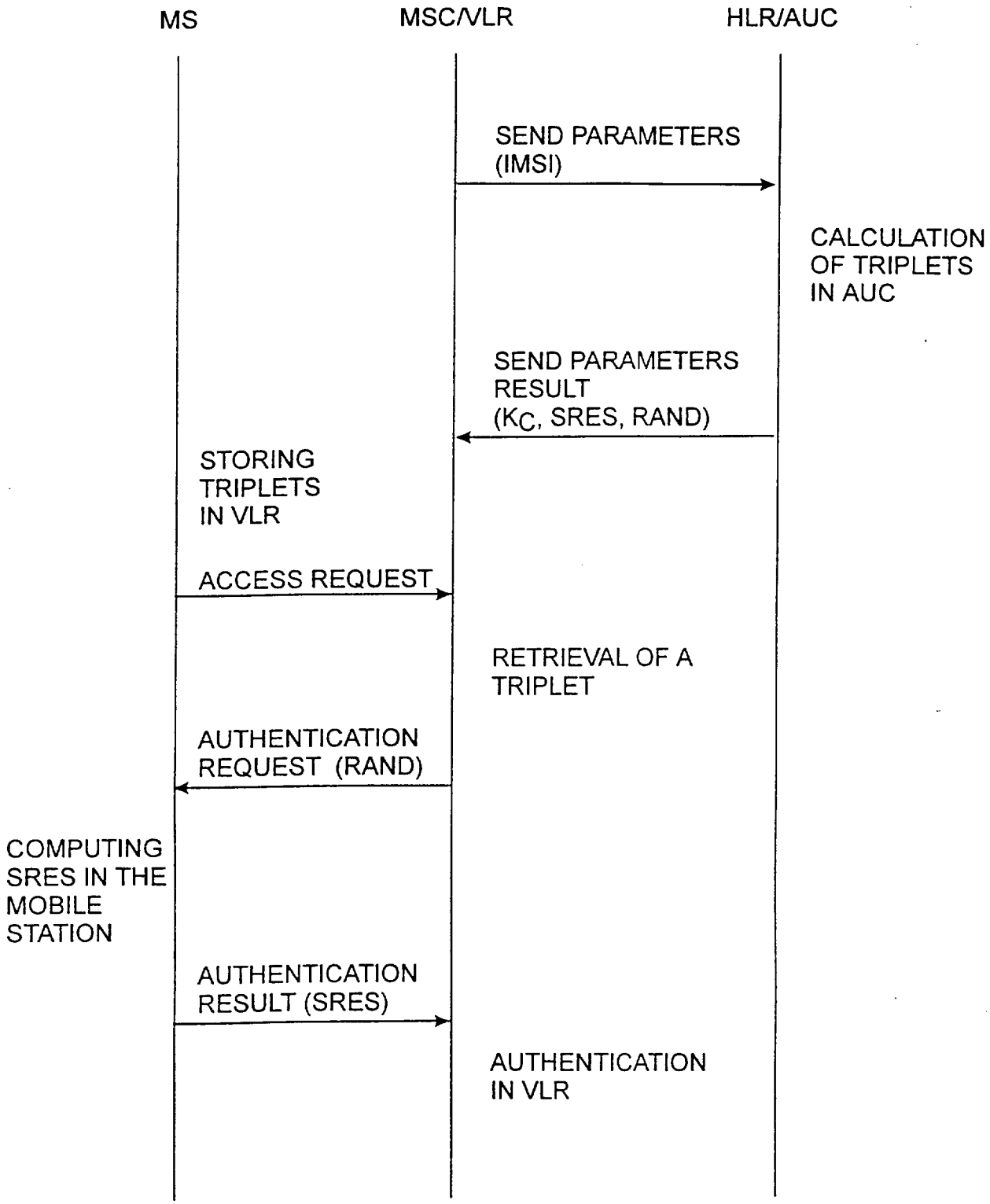


Fig. 6

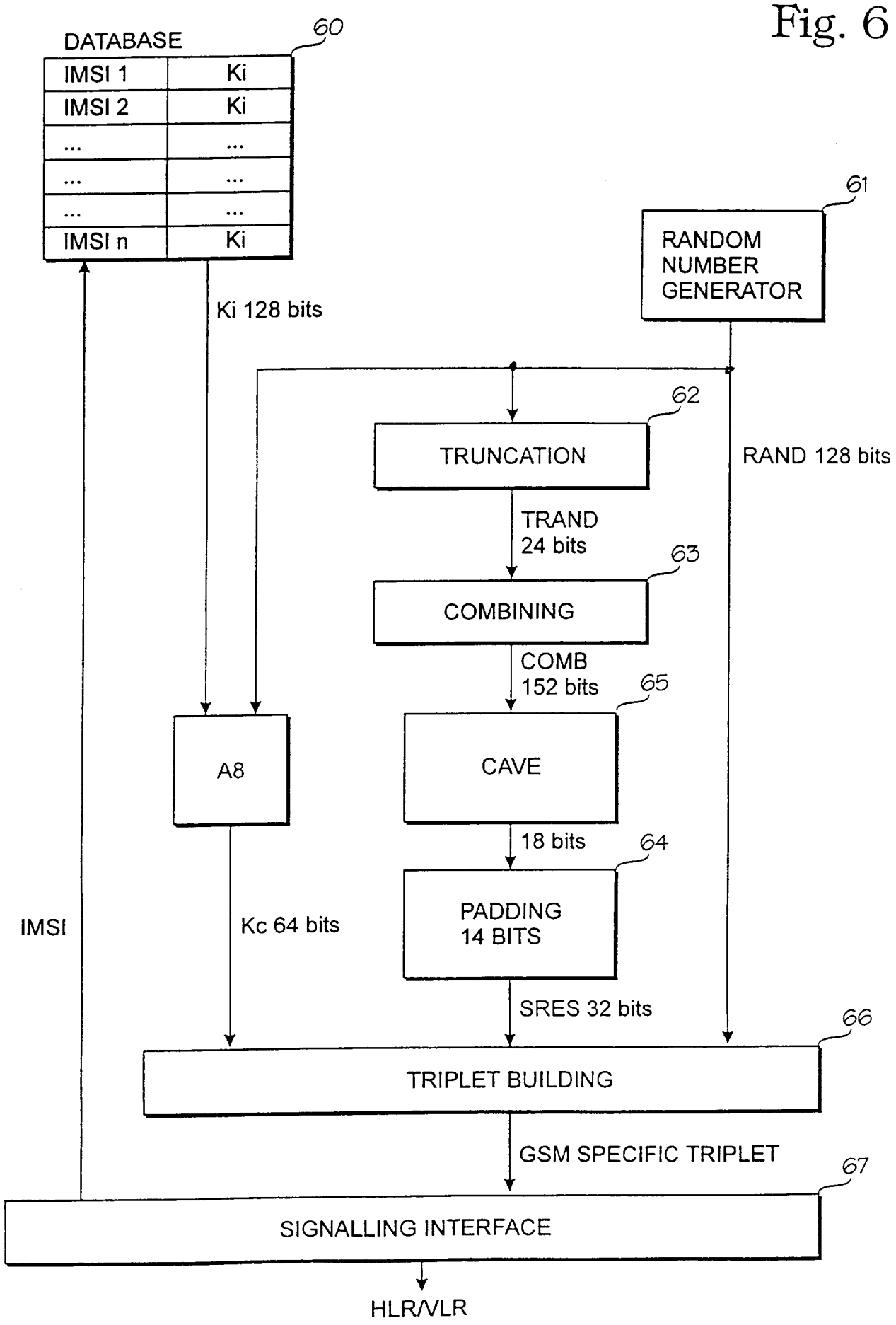

DATABASE
60
IMSI 1
Ki
IMSI 2
Ki
...
...
...
...
...
...
IMSI n
Ki
61
RANDOM NUMBER GENERATOR
Ki 128 bits
62
TRUNCATION
RAND 128 bits
TRAND 24 bits
63
COMBINING
COMB 152 bits
65
A8
CAVE
18 bits
64
PADDING 14 BITS
IMSI
Kc 64 bits
SRES 32 bits
66
TRIPLET BUILDING
GSM SPECIFIC TRIPLET
67
SIGNALLING INTERFACE
HLR/VLR

Fig. 7

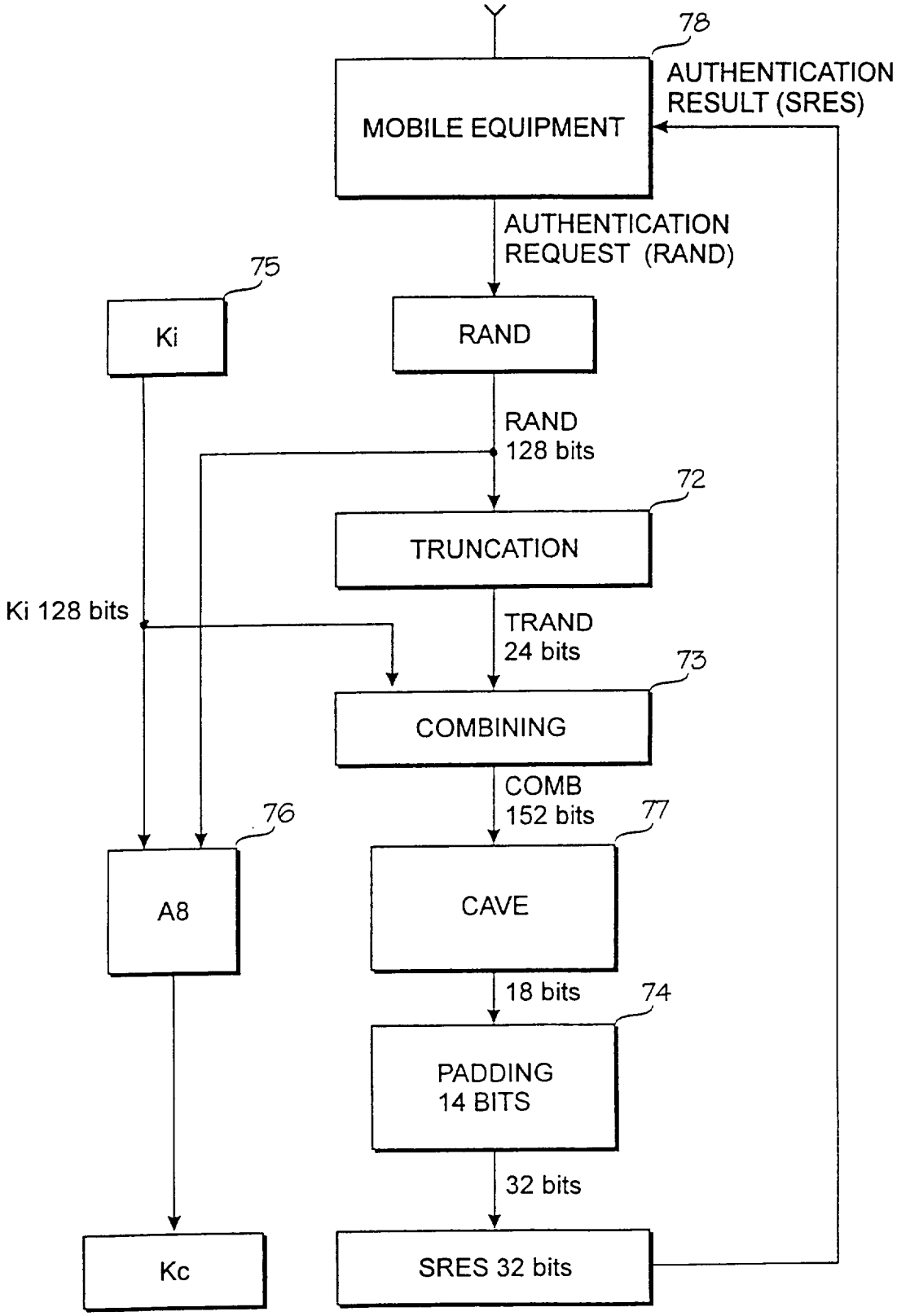
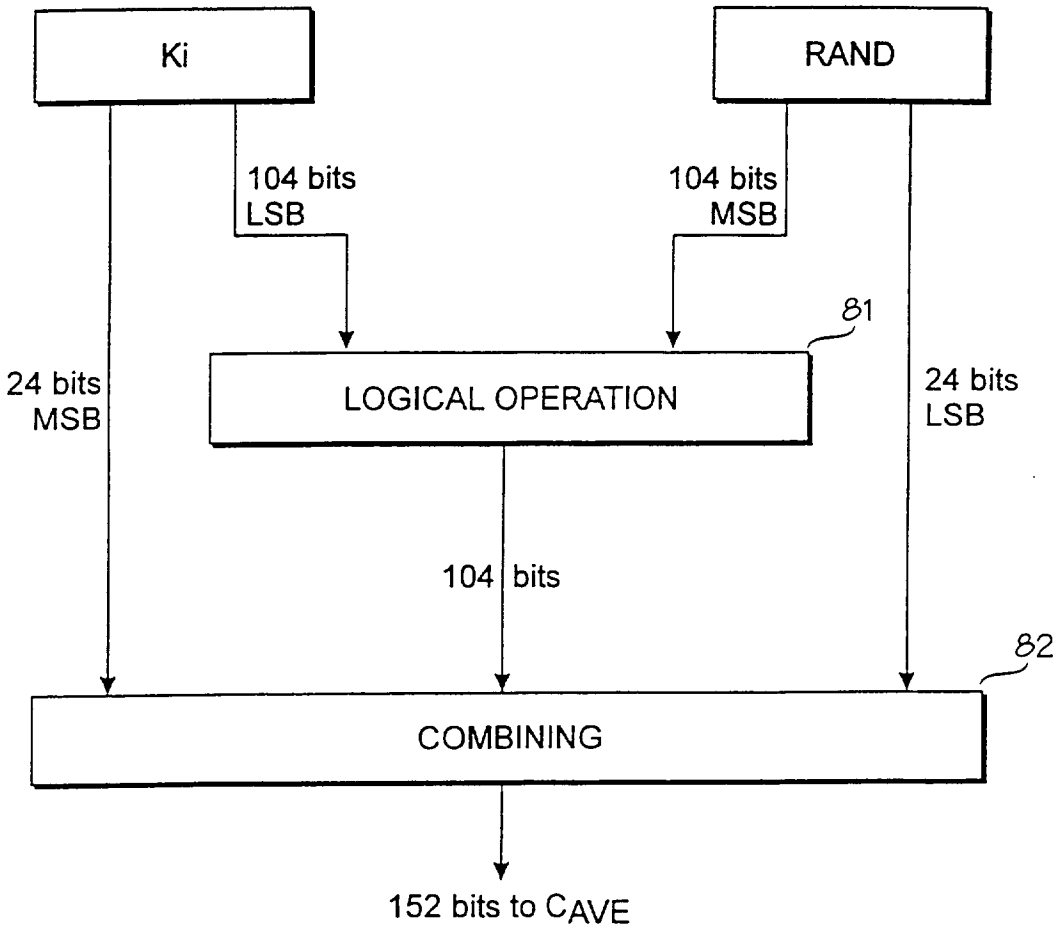

78
AUTHENTICATION RESULT (SRES)
MOBILE EQUIPMENT
AUTHENTICATION REQUEST (RAND)
75
Ki
RAND
RAND 128 bits
72
TRUNCATION
Ki 128 bits
TRAND 24 bits
73
COMBINING
COMB 152 bits
76
77
A8
CAVE
18 bits
74
PADDING 14 BITS
32 bits
Kc
SRES 32 bits

Fig. 8


Ki
RAND
104 bits
LSB
104 bits
MSB
81
24 bits
MSB
LOGICAL OPERATION
24 bits
LSB
104 bits
82
COMBINING
152 bits to CAVE

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 96/00543

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 7/38, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0675615 A1 (FRANCE TELECOM), 4 October 1995 (04.10.95), abstract --	1-8
A	US 5319710 A (M. ATALLA ET AL), 7 June 1994 (07.06.94), column 2, line 49 - column 6, line 16 --	1-8
P,A	US 5513245 A (S.MIZIKOVSKY ET AL.), 30 April 1996 (30.04.96), column 3, line 46 - column 4, line 26 -- --------	1-8

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 March 1997	20 -03- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Christina Halldin Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

03/02/97

International application No.
PCT/FI 96/00543

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A1- 0675615	04/10/95	FR-A,B- 2718312	06/10/95
		JP-A- 8008899	12/01/96
US-A- 5319710	07/06/94	AU-A- 664823	07/12/95
		EP-A- 0678836	25/10/95
US-A- 5513245	30/04/96	NONE	